

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-118975

(43)Date of publication of application : 15.04.2004

(51)Int.Cl.

G11B	20/10
G06F	12/14
G06F	17/60
G11B	33/06
H04L	9/10
H04N	5/91
H04N	7/167

(21)Application number : 2002-283862

(71)Applicant : NIPPON TELEGR & TELEPH CORP
 <NTT>

(22)Date of filing : 27.09.2002

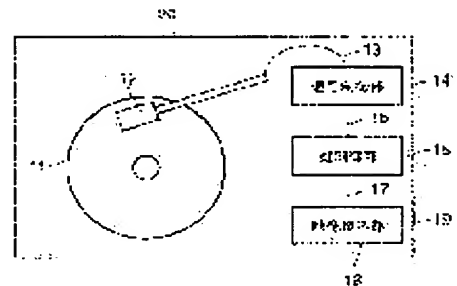
(72)Inventor : KISHIGAMI JUNICHI
YAMAGUCHI MASAYASU
KAWAZOE KATSUHIKO

(54) ACCUMULATING SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an accumulating system in which suppression of an illegal copy can be realized easily by preventing the decoded signal of contents from being leaked to the outside of a case and by exposing no key to the outside of the case.

SOLUTION: This system is provided with a recording medium 11 in which a ciphered signal of contents can be recorded and an ID signal is recorded, a head 12 which can record and reproduce a signal electromagnetically in the recording medium 11, a magnetic disk device having a mechanism which can shift the head 12 to the prescribed position, a signal control section 14 extracting the ciphered signal of contents and the ID signal from the recording medium 11, a key control section 16 decoding the ciphered signal of contents from the prescribed medium by mutual action of the ID signal from the signal control section 14 and the key of cipher previously obtained, and a video demodulation section 18 demodulating the video signal decoded by the key control section 16 and outputting an analog signal to a display.



(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2004-118975

(P2004-118975A)

(43) 公開日 平成16年4月15日 (2004.4.15)

(51) Int. Cl. ⁷

F I

テーマコード (参考)

G 1 1 B 20/10

G 1 1 B 20/10

H

5 B 0 1 7

G 0 6 F 12/14

G 1 1 B 20/10

3 0 1 Z

5 C 0 5 3

G 0 6 F 17/60

G 0 6 F 12/14

3 2 0 B

5 C 0 6 4

G 1 1 B 33/06

G 0 6 F 12/14

3 2 0 D

5 D 0 4 4

H 0 4 L 9/10

G 0 6 F 17/60

3 0 2 E

5 J 1 0 4

審査請求 未請求 請求項の数 4 O L (全 7 頁) 最終頁に続く

(21) 出願番号

特願2002-283862 (P2002-283862)

(22) 出願日

平成14年9月27日 (2002.9.27)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(74) 代理人 100058479

弁理士 鈴江 武彦

(74) 代理人 100084618

弁理士 村松 貞男

(74) 代理人 100087963

弁理士 石川 義雄

(72) 発明者 岸上 順一

東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

(72) 発明者 山口 正泰

東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

最終頁に続く

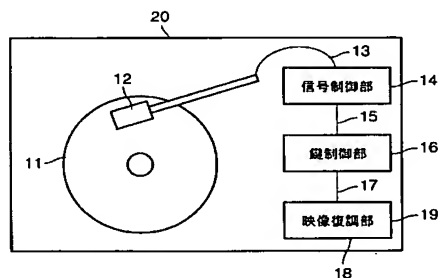
(54) 【発明の名称】 蓄積システム

(57) 【要約】

【課題】本発明の課題は、鍵が筐体外にさらされることがなく、解読されたコンテンツの信号が筐体外に出ないことにより容易に不正コピーの抑止を実現できる蓄積システムを提供することにある。

【解決手段】本発明は、暗号化されたコンテンツの信号が記録できると共に I D の信号が記録された記録媒体 1 1 と、記録媒体 1 1 に電磁的に信号を記録再生できるヘッド 1 2 と、ヘッド 1 2 を所定の位置に移動できる機構を有する磁気ディスク装置と、記録媒体 1 1 から暗号化されたコンテンツの信号と I D の信号を抽出する信号制御部 1 4 と、信号制御部 1 4 からの I D の信号と予め取得した暗号の鍵との相互作用により所定の媒体からの暗号化されたコンテンツの信号を解読する鍵制御部 1 6 と、鍵制御部 1 6 で解読された映像信号を復調してアナログ信号を表示部に出力する映像復調部 1 8 とが同一の筐体 2 0 内に設けられる。

【選択図】 図 1



【特許請求の範囲】

【請求項 1】

暗号化されたコンテンツの信号が記録できると共に I D の信号が記録された媒体と、該媒体に電磁的に信号を記録再生できるヘッドと、該ヘッドを所定の位置に移動できる機構を有する磁気ディスク装置と、
前記媒体から暗号化されたコンテンツの信号と I D の信号を抽出する信号制御部と、
該信号制御部からの I D の信号と予め取得した暗号の鍵との相互作用により所定の媒体からの暗号化されたコンテンツの信号を解読する鍵制御部と、
該鍵制御部で解読された映像信号を復調してアナログ信号を表示部に出力する映像復調部とが同一の筐体内に設けられることを特徴とする蓄積システム。

10

【請求項 2】

請求項 1 記載の蓄積システムにおいて、鍵制御部として解読されたコンテンツの信号の圧縮を解く回路を含むことを特徴とする蓄積システム。

【請求項 3】

請求項 1 又は 2 記載の蓄積システムにおいて、筐体を開放すると、媒体の記録再生が行えなくなることを特徴とする蓄積システム。

【請求項 4】

請求項 1、2 又は 3 記載の蓄積システムにおいて、ヘッドのヘッド部もしくはジンバル部を筐体に接続部で接続し、筐体を開放するとヘッドが移動して媒体の記録再生が行えなくなることを特徴とする蓄積システム。

20

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、例えば映像、音楽などの大容量のコンテンツを暗号を用いて安全に蓄積し、外部からの不正なアクセスにより暗号化されたコンテンツを解読することが不可能にせしめる蓄積システムに関するものである。

【0002】

【従来の技術】

磁気ディスクの大容量化に伴い、安価で使いやすい蓄積装置としての地位はますます強くなってきている。従来はコンピュータデータの主たる蓄積装置であったが、近年は音楽や映像などの大容量のコンテンツの蓄積にまでその応用範囲が広がってきている。また、コンテンツがデジタル化されコピーや移動が安価で手軽に行えることになったことにより、不正な使用が顕在化してきている。さらに最近では磁気ディスク内蔵の録画装置が売り出され、この録画装置を用いた新しいサービスも検討されている。これらのサービスにおいてコンテンツの不正コピーなどを防ぐ目的から、送り手においてコンテンツを暗号化し、蓄積装置を内蔵した受信装置において鍵を用いて暗号を解く方法が考えられている。ここで最も重要になるのはコンテンツの暗号を解く鍵が外部にさらされることである。暗号の強度をいくら上げたとしても、蓄積装置を内蔵した受信装置までにその暗号を解く鍵が盗まれるとコンテンツは簡単にコピーされてしまうからである。現在の衛星デジタル放送では放送という特定の環境が保証されているため、カードに鍵の元になる信号を記録しておき、それをベースに送られてくる暗号化されたコンテンツを解く方法などが使われている。しかし厳密に見るとこの方法でもカードと回路あるいは蓄積装置との間で鍵のやり取りが行われるため、そこが一種のセキュリティホールになることが指摘されている。またデジタル化されている信号は通常何らかの圧縮が行われているため、まず暗号を解き、その後圧縮を解く回路にコンテンツ信号が送られる。ここでも生のコンテンツ信号が盗まれる可能性がある。

30

40

【0003】

このようなデータのセキュリティに係る公知文献として、特許文献 1 のデータ記録再生装置及びセキュリティ管理方法、特許文献 2 のデータセキュリティ装置、及び特許文献 3 のネットワークに直接接続可能なディスク装置があるが、いずれも磁気ディスクのコン

50

トローラへのアクセスを安全にするもので、磁気ディスクそのものを安全にするものではない。

【0004】

【特許文献1】

特開平10-97468号公報

【特許文献2】

特開平8-185349号公報

【特許文献3】

特開2000-347808号公報

【発明が解決しようとする課題】

本発明は上記の事情に鑑みてなされたもので、予め暗号の鍵を取得して暗号化されたコンテンツの信号を解読する鍵制御部を磁気ディスク装置と同一筐体内に設け、筐体を開放すると媒体の記録再生が行えなくなるようにすることにより、鍵が筐体外にさらされることがなく、解読されたコンテンツの信号が筐体外に出ないことにより容易に不正コピーの抑止を実現できる蓄積システムを提供することを目的とする。

【0005】

【課題を解決するための手段】

上記目的を達成するために本発明の蓄積システムは、暗号化されたコンテンツの信号が記録できると共にIDの信号が記録された媒体と、該媒体に電磁的に信号を記録再生できるヘッドと、該ヘッドを所定の位置に移動できる機構を有する磁気ディスク装置と、前記媒体から暗号化されたコンテンツの信号とIDの信号を抽出する信号制御部と、該信号制御部からのIDの信号と予め取得した暗号の鍵との相互作用により所定の媒体からの暗号化されたコンテンツの信号を解読する鍵制御部と、該鍵制御部で解読された映像信号を復調してアナログ信号を表示部に出力する映像復調部とが同一の筐体内に設けられることを特徴とするものである。

【0006】

また本発明は、前記蓄積システムにおいて、鍵制御部として解読されたコンテンツの信号の圧縮を解く回路を含むことを特徴とするものである。

【0007】

また本発明は、前記蓄積システムにおいて、筐体を開放すると、媒体の記録再生が行えなくなることを特徴とするものである。

【0008】

また本発明は、前記蓄積システムにおいて、ヘッドのヘッド部もしくはジンバル部を筐体に接続部で接続し、筐体を開放するとヘッドが移動して媒体の記録再生が行えなくなることを特徴とするものである。

【0009】

【発明の実施の形態】

以下図面を参照して本発明の実施の形態例を詳細に説明する。

【0010】

図1は本発明の実施形態例に係る蓄積システムを示す構成説明図である。11は例えば磁気ディスク等の記録媒体であり、この記録媒体11には暗号化されたコンテンツの信号が記録されると共にIDの信号が記録される。コンテンツを発信する側である、プロバイダーにおいては自らのコンテンツの不正使用を防止するため、一定の決まりに基づいてコンテンツの信号に暗号化がされている。蓄積装置を内蔵した受信装置においてこの暗号化されたコンテンツの信号を受信した後、そのまま記録媒体11に記録される。また記録媒体11には個別の装置毎に再生を制御するためのIDの信号が例えば磁気ディスク装置に用いられているサーボ信号の一部に重畳するなどの方法により容易に消去あるいは書き換えができないように記録される。12は記録媒体11に電磁的に信号を記録再生できるヘッド部及びジンバル部よりなるヘッドであり、このヘッド12には所定の位置に移動できるヘッド移動機構（図示せず）が設けられる。このヘッド移動機構、記録媒体11、及びヘ

10

20

30

40

50

ッド12より磁気ディスク装置が構成される。前記ヘッド12には第1のインターフェース13を介して信号制御部14が接続される。信号制御部14では記録媒体11からの暗号化されたコンテンツの信号とIDの信号が抽出され、第2のインターフェース15を介して鍵制御部16に出力される。鍵制御部16は信号制御部14からの記録媒体11のIDの信号と予め取得した暗号の鍵との相互作用により所定の記録媒体11からの暗号化されたコンテンツの信号を解読して復号化する。暗号化においてはあらかじめ決められたアルゴリズムが鍵制御部16にあり、コンテンツに重畳あるいは別の手段によって送られてきた鍵の信号と受け手の記録媒体11からのIDの信号との相互作用により正しく視聴が許可された磁気ディスク装置の記録媒体11でのみ再生を実現するものである。鍵制御部16には鍵のやり取りをする回路及びコンテンツの信号の圧縮を解く回路が含まれる。コンテンツの信号が映像を示す信号の場合は、鍵制御部16で暗号を解読した後圧縮を解いたコンテンツの映像信号が第3のインターフェース17を介して映像復調部18に入力される。映像復調部18では暗号を解読した後圧縮を解いたコンテンツの映像信号をアナログ信号に復調し、このコンテンツの映像アナログ信号を第4のインターフェース19を介して表示部（図示せず）に出力される。前記磁気ディスク装置、信号制御部14、鍵制御部16、及び映像復調部18は同一の例えば箱等の筐体20の内部に配設される。前記信号制御部14、鍵制御部16、及び映像復調部18はチップあるいは回路として実装される。第4のインターフェース19までの信号はすべて容易には外部から触れない筐体20の中で処理される。もし不正を行おうとする場合はこの筐体20を開放しなければならないが、記録媒体11の磁気ディスクはヘッド12と数十ナノメートルという間隔で離れていなければならないため、ゴミのない非常にクリーンな環境でなければ開放できない。もし、通常的环境下で開放された場合はクラッシュという現象を起こし、それ以降記録再生が不可能になる。またより積極的に磁気ディスク装置の記録再生を不可能にするためには、筐体20を開放した途端、ヘッド12が通常位置からずれる機構をもつようにしてもよい。

【0011】

図2は本発明の実施形態例に係る磁気ディスク装置を示す構成説明図である。すなわち、ヘッド12のヘッド部21は筐体20に接続部22で接続されている。23はヘッド12のジンバル部である。ここで筐体20を開放しようとするすると筐体20に接続されている接続部22によりヘッド部21に移動などの影響が出る。これにより以降の記録再生が不可能になる。図2ではあたかも記録媒体11とヘッド12が一つしかないように書かれているが、実際には複数ある場合もある。その場合でも接続部22は有効である。直接ヘッド部21に接続することが不可能であればそれを支えるジンバル部23に接続されていても同じ効果が得られる。

【0012】

このように、予め暗号の鍵を取得して暗号化されたコンテンツの信号を解読する鍵制御部を磁気ディスク装置と同一筐体内に設け、筐体を開放すると記録媒体の記録再生が行えなくなるようにすることにより、鍵が筐体外にさらされることがなく、解読されたコンテンツの信号が筐体外に出ないことにより容易に不正コピーの抑止を実現できる。

【0013】

図3は本発明の実施形態例に係る蓄積システムを通信放送融合サービスのビジネスモデルに応用した例を示す説明図である。すなわち、コンテンツ配信事業会社31はメタデータデータベース（DB）を有してメタデータ管理サービスを行なうと共に、地域IP網、アクセス網32を用いてコンテンツ配信サービスを行なう。コンテンツ配信事業会社31は放送局33、広告マーケティングを行う広告会社34、メタデータデータベース（DB）を有しコンテンツ資産管理（Asset Management）を行うコンテンツ制作会社35とメタデータの通信を行う。放送局33はコンテンツ配信事業会社31にコンテンツ配送手数料を払ってコンテンツを供給し、広告会社34はコンテンツ配信事業会社31にマーケティング料を払ってコンテンツを供給し、コンテンツ制作会社35はコンテンツ配信事業会社31に資産管理手数料を払ってコンテンツを供給する。コンテンツ配信事

10

20

30

40

50

業会社 31 はユーザ 36 とメタデータの通信を行い、ユーザ 36 にコンテンツを提供すると共にユーザ 36 からコンテンツ配信利用料を徴収する。尚、ユーザ 36 は放送局 33 にコンテンツ利用料を支払う場合もある。

【0014】

コンテンツ配信事業会社 31 からユーザ 36 に提供されたコンテンツはゲートウェイ 37 を介して STB (Set Top Box) または PDR (Personal Digital Recorder) 38 に入力され、本発明の実施形態例に係る蓄積システム 39 に記録される。この場合、蓄積システム 39 はユーザプロファイル (ログ情報) としても使用される。蓄積システム 39 に記録されたコンテンツを再生する場合はパソコン (PC) 40 を用いて行われる。

10

【0015】

【発明の効果】

以上述べたように本発明によれば、暗号化されて蓄積されているコンテンツの解読において、外部からは容易に解読された信号にアクセスすることが困難な方式を内包した磁気ディスク装置であり、コンテンツを安全に蓄積することを実現し、蓄積を前提としたコンテンツ配信サービスに用いられるものである。

【図面の簡単な説明】

【図 1】 本発明の実施形態例に係る蓄積システムを示す構成説明図である。

【図 2】 本発明の実施形態例に係る磁気ディスク装置を示す構成説明図である。

【図 3】 本発明の実施形態例に係る蓄積システムを通信放送融合サービスのビジネスモデルに応用した例を示す説明図である。

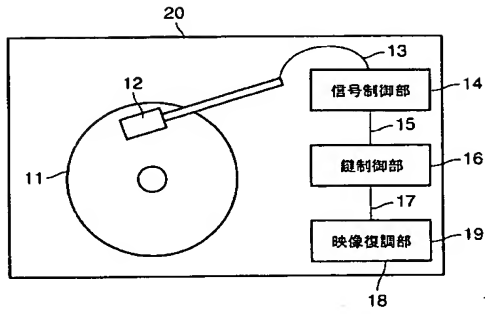
20

【符号の説明】

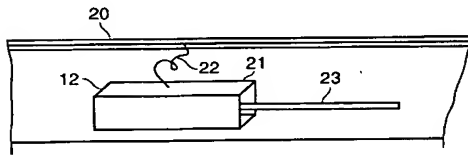
- 11 記録媒体
- 12 ヘッド
- 13 第 1 のインターフェース
- 14 信号制御部
- 15 第 2 のインターフェース
- 16 鍵制御部
- 17 第 3 のインターフェース
- 18 映像復調部
- 19 第 4 のインターフェース
- 20 筐体

30

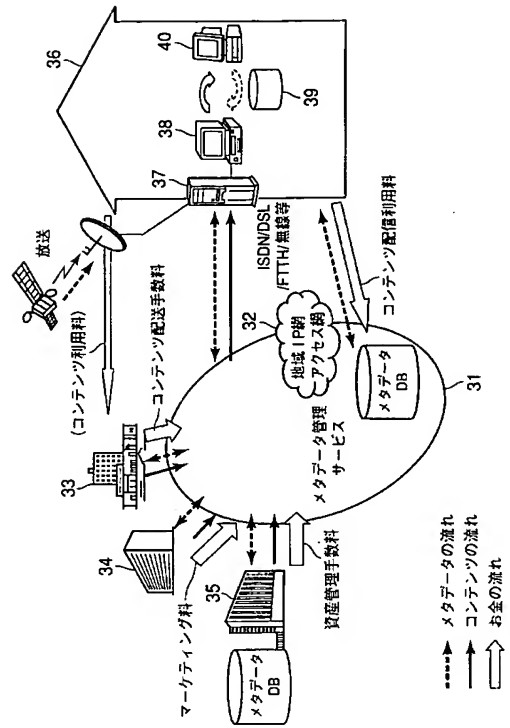
【図 1】



【図 2】



【図 3】



フロントページの続き

(51)Int.Cl.⁷

H O 4 N 5/91
H O 4 N 7/167

F I

G O 6 F 17/60 5 1 2
G 1 1 B 33/06 M
H O 4 N 5/91 P
H O 4 L 9/00 6 2 1 A
H O 4 N 7/167 Z

テーマコード (参考)

(72)発明者 川添 雄彦

東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

Fターム(参考) 5B017 AA03 AA07 BA07 BA08 CA07 CA16

5C053 FA13 FA23 GB21 JA21 KA25 LA06 LA07

5C064 CA14 CA18 CB01

5D044 AB07 BC01 CC05 DE50 DE54 GK12 GK17 HL08

5J104 AA12 AA16 AA45 EA09 NA02 NA31 NA42 NA43 PA14